

Lifting Constructions of Strongly Regular Cayley Graphs

Koji Momihara* Qing Xiang†

Abstract

We give two “lifting” constructions of strongly regular Cayley graphs. In the first construction we “lift” a cyclotomic strongly regular graph by using a subdifference set of the Singer difference set. The second construction uses quadratic forms over finite fields and it is a common generalization of the construction of the affine polar graphs [7] and a construction of strongly regular Cayley graphs given in [15]. The two constructions are related in the following way: The second construction can be viewed as a recursive construction, and the strongly regular Cayley graphs obtained from the first construction can serve as starters for the second construction. We also obtain association schemes from the second construction.

Keywords: Cyclotomic strongly regular graph, Gauss sum, quadratic form, strongly regular graph.

1 Introduction

In this paper, we assume that the reader is familiar with the theory of strongly regular graphs and difference sets. For the theory of strongly regular graphs, our main references are [5] and [18]. For the theory of difference sets, we refer the reader to Chapter 6 of [4]. Strongly regular graphs (srgs) are closely related to other combinatorial objects, such as two-weight codes, two-intersection sets in finite geometry, and partial difference sets. For these connections, we refer the reader to [5, p. 132] and [7, 22].

Let Γ be a simple and undirected graph and A be its adjacency matrix. A very useful way to check whether Γ is strongly regular is by using the eigenvalues of A (which are usually called eigenvalues of Γ). For convenience, we will call an eigenvalue of Γ *restricted* if it has an eigenvector perpendicular to the all-ones vector $\mathbf{1}$. Note that for a k -regular connected graph, the restricted eigenvalues are simply the eigenvalues different from k .

Theorem 1.1. *For a simple k -regular graph Γ of order v , not complete or edgeless, with adjacency matrix A , the following are equivalent:*

1. Γ is strongly regular with parameters (v, k, λ, μ) for certain integers λ, μ ,
2. $A^2 = (\lambda - \mu)A + (k - \mu)I + \mu J$ for certain real numbers λ, μ , where I, J are the identity matrix and the all-ones matrix, respectively,
3. A has precisely two distinct restricted eigenvalues.

One of the most effective methods for constructing srgs is by the Cayley graph construction. For example, the Paley graph $P(q)$ is a class of well-known Cayley graphs on the finite field \mathbb{F}_q ; that

*Department of Mathematics, Faculty of Education, Kumamoto University, 2-40-1 Kurokami, Kumamoto 860-8555, Japan; Email: momihara@educ.kumamoto-u.ac.jp

†Department of Mathematical Science, University of Delaware, Newark, DE 19716, USA; Email: xiang@math.udel.edu

is, the vertices of $P(q)$ are the elements of \mathbb{F}_q , and two vertices are adjacent if and only if their difference is a nonzero square. The parameters of $P(q)$ are $(v, k, \lambda, \mu) = (4t + 1, 2t, t - 1, t)$, where $q = 4t + 1$ is a prime power. More generally, let G be an additively written group of order v , and let D be a subset of G such that $0 \notin D$ and $-D = D$, where $-D = \{-d \mid d \in D\}$. The *Cayley graph on G with connection set D* , denoted by $\text{Cay}(G, D)$, is the graph with the elements of G as vertices; two vertices are adjacent if and only if their difference belongs to D . In the case where $\text{Cay}(G, D)$ is strongly regular, the connection set D is called a (regular) *partial difference set*. The survey of Ma [22] contains much of what is known about partial difference sets and about connections with strongly regular Cayley graphs.

A classical method for constructing strongly regular Cayley graphs on the additive groups of finite fields is to use cyclotomic classes of finite fields. Let p be a prime, f a positive integer, and let $q = p^f$. Let $e > 1$ be an integer such that $e \mid (q - 1)$, and γ be a primitive element of \mathbb{F}_q . Then the cosets $C_i^{(e,q)} = \gamma^i \langle \gamma^e \rangle$, $0 \leq i \leq e - 1$, are called the *cyclotomic classes of order e* of \mathbb{F}_q . Many authors have studied the problem of determining when a union D of cyclotomic classes forms a partial difference set. We call $\text{Cay}(\mathbb{F}_q, D)$ a *cyclotomic strongly regular graph* if D is a single cyclotomic class of \mathbb{F}_q and $\text{Cay}(\mathbb{F}_q, D)$ is strongly regular. Extensive work has been done on cyclotomic srgs, see [2, 6, 14, 16, 17, 19, 21, 23, 25, 26, 27]. (Some of these authors used the language of cyclic codes in their investigations instead of strongly regular Cayley graphs or partial difference sets. We choose to use the language of srgs here.) The Paley graphs are primary examples of cyclotomic srgs. Also, if D is the multiplicative group of a subfield of \mathbb{F}_q , then it is clear that $\text{Cay}(\mathbb{F}_q, D)$ is strongly regular. These cyclotomic srgs are usually called *subfield examples*. Next, if there exists a positive integer t such that $p^t \equiv -1 \pmod{e}$, then $\text{Cay}(\mathbb{F}_q, D)$ is strongly regular. See [2]. These examples are usually called *semi-primitive*. Schmidt and White made the following conjecture on cyclotomic srgs.

Conjecture 1.2. ([26]) *Let \mathbb{F}_{p^f} be the finite field of order p^f , $e \mid \frac{p^f - 1}{p - 1}$ with $e > 1$, and $C_0 = C_0^{(e,p^f)}$ with $-C_0 = C_0$. If $\text{Cay}(\mathbb{F}_{p^f}, C_0)$ is strongly regular, then one of the following holds:*

- (1) (*subfield case*) $C_0 = \mathbb{F}_{p^d}^*$ where $d \mid f$,
- (2) (*semi-primitive case*) $-1 \in \langle p \rangle \leq (\mathbb{Z}/e\mathbb{Z})^*$,
- (3) (*exceptional case*) $\text{Cay}(\mathbb{F}_{p^f}, C_0)$ has one of the eleven sets of parameters given in Table 1.

Table 1: Eleven sporadic examples

No.	e	p	f	$[(\mathbb{Z}/e\mathbb{Z})^* : \langle p \rangle]$
1	11	3	5	2
2	19	5	9	2
3	35	3	12	2
4	37	7	9	4
5	43	11	7	6
6	67	17	33	2
7	107	3	53	2
8	133	5	18	6
9	163	41	81	2
10	323	3	144	2
11	499	5	249	2

A strongly regular graph is said to be of *Latin square type* (respectively, *negative Latin square type*) if $(v, k, \lambda, \mu) = (n^2, r(n - \epsilon), \epsilon n + r^2 - 3\epsilon r, r^2 - \epsilon r)$ and $\epsilon = 1$ (respectively, $\epsilon = -1$). Typical examples

of srgs of Latin square type or negative Latin square type come from nonsingular quadrics in the projective space $\text{PG}(m-1, q)$, where m is even. It seems that we know more examples of srgs of Latin square type than srgs of negative Latin square type, see [10]. Our first main result in this paper is a construction of negative Latin square type strongly regular Cayley graphs $\text{Cay}(\mathbb{F}_{q^2}, D)$ by lifting a cyclotomic strongly regular graph on \mathbb{F}_q . The proof relies on the Davenport-Hasse lifting formula on Gauss sums.

In our second main theorem, we will give a recursive construction of strongly regular Cayley graphs by using quadratic forms over finite fields under the assumption that certain strongly regular Cayley graphs exist on a ground field. This construction generalizes the following two constructions.

Theorem 1.3. ([7]) *Let $Q : V = \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ be a nonsingular quadratic form, where n is even and q is an odd prime power, and let $D = \{x \in \mathbb{F}_q^n \mid Q(x) \text{ is a nonzero square in } \mathbb{F}_q\}$. Then, $\text{Cay}(V, D)$ is a strongly regular graph (which is the so-called affine polar graph).*

Feng et.al [15] gave the following construction using uniform cyclotomy.

Theorem 1.4. ([15]) *Let p be a prime, $e > 2$, $q = p^{2jr}$, where $r \geq 1$, $e \mid (p^j + 1)$, and j is the smallest such positive integer. Let $Q : V = \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ be a nonsingular quadratic form, where n is even, and let $D_{C_i^{(e,q)}} = \{x \in \mathbb{F}_q^n \mid Q(x) \in C_i^{(e,q)}\}$ for $0 \leq i \leq e-1$. Then, $\text{Cay}(V, D_{C_i^{(e,q)}})$ is strongly regular for all $0 \leq i \leq e-1$.*

The strongly regular Cayley graphs obtained in Section 3 can be used as starters for the second construction. In this way, we obtain a few infinite families of strongly regular Cayley graphs with Latin square type or negative Latin square type parameters. Furthermore, we discuss association schemes related to the second construction and obtain several new association schemes.

2 Background on Gauss sums and strongly regular Cayley graphs

Let p be a prime, f a positive integer, and $q = p^f$. The canonical additive character ψ of \mathbb{F}_q is defined by

$$\psi : \mathbb{F}_q \rightarrow \mathbb{C}^*, \quad \psi(x) = \zeta_p^{\text{Tr}_{q/p}(x)},$$

where $\zeta_p = \exp(\frac{2\pi i}{p})$ is a complex primitive p -th root of unity and $\text{Tr}_{q/p}$ is the trace from \mathbb{F}_q to \mathbb{F}_p . All complex characters of $(\mathbb{F}_q, +)$ are given by ψ_a , where $a \in \mathbb{F}_q$. Here ψ_a is defined by

$$\psi_a(x) = \psi(ax), \quad \forall x \in \mathbb{F}_q. \quad (2.1)$$

For a multiplicative character χ_e of order e of \mathbb{F}_q , we define the *Gauss sum*

$$G_f(\chi_e) = \sum_{x \in \mathbb{F}_q^*} \chi_e(x) \psi(x).$$

From the definition we see clearly that $G_f(\chi_e) \in \mathbb{Z}[\zeta_{ep}]$, the ring of algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta_{ep})$. Let $\sigma_{a,b}$ be the automorphism of $\mathbb{Q}(\zeta_{ep})$ defined by

$$\sigma_{a,b}(\zeta_e) = \zeta_e^a, \quad \sigma_{a,b}(\zeta_p) = \zeta_p^b,$$

where $\gcd(a, e) = \gcd(b, p) = 1$. Below we list several basic properties of Gauss sums [3]:

- (i) $G_f(\chi_e) \overline{G_f(\chi_e)} = q$ if χ_e is nontrivial;

- (ii) $G_f(\chi_e^p) = G_f(\chi_e)$, where p is the characteristic of \mathbb{F}_q ;
- (iii) $G_f(\chi_e^{-1}) = \chi_e(-1)\overline{G_f(\chi_e)}$;
- (iv) $G_f(\chi_e) = -1$ if χ_e is trivial;
- (v) $\sigma_{a,b}(G_f(\chi_e)) = \chi_e^{-a}(b)G_f(\chi_e^a)$.

In general, explicit evaluations of Gauss sums are very difficult. There are only a few cases where the Gauss sums have been evaluated. The most well-known case is the *quadratic* case, i.e., the order of χ_e is two. The next simple case is the so-called *semi-primitive case* (also known as *uniform cyclotomy* or *pure Gauss sum*), where there exists an integer j such that $p^j \equiv -1 \pmod{e}$, where e is the order of the multiplicative character involved. The explicit evaluations of Gauss sums in these cases are given in [3]. The next interesting case is the index 2 case where the subgroup $\langle p \rangle$ generated by $p \in (\mathbb{Z}/e\mathbb{Z})^*$ is of index 2 in $(\mathbb{Z}/e\mathbb{Z})^*$ and $-1 \notin \langle p \rangle$. In this case, it is known that e can have at most two odd prime divisors. Many authors have investigated this case, see [29] for a complete solution to the problem of evaluating index 2 Gauss sums. Recently, these index 2 Gauss sums were used in the construction of new infinite families of strongly regular graphs. See [14, 16].

Now we recall the following well-known lemma in algebraic graph theory (see e.g., [5]).

Lemma 2.1. *Let $(G, +)$ be an abelian group and D a subset of G such that $0 \notin D$ and $D = -D$. Then, the restricted eigenvalues of $\text{Cay}(G, D)$ are given by $\psi(D)$, $\psi \in \widehat{G} \setminus \{\psi_0\}$, where \widehat{G} is the character group of G and ψ_0 is the trivial character.*

Let q be a prime power and let $C_i^{(e,q)} = \gamma^i \langle \gamma^e \rangle$, $0 \leq i \leq e-1$, be the cyclotomic classes of order e of \mathbb{F}_q , where γ is a fixed primitive root of \mathbb{F}_q . In order to check whether a candidate subset $D = \bigcup_{i \in I} C_i^{(e,q)}$ is a connection set of a strongly regular Cayley graph, by Theorem 1.1 and Lemma 2.1, it is enough to show that $\psi(aD) = \sum_{x \in D} \psi(ax)$, $a \in \mathbb{F}_q^*$, take exactly two values, where ψ is the canonical additive character of \mathbb{F}_q . Note that the sum $\psi(aD)$ can be expressed as a linear combination of Gauss sums (cf. [16]) by using the orthogonality of characters:

$$\psi(aD) = \frac{1}{e} \sum_{\chi \in C_0^\perp} G_f(\chi^{-1}) \sum_{i \in I} \chi(a\gamma^i), \quad (2.2)$$

where C_0^\perp is the subgroup of $\widehat{\mathbb{F}_q^*}$ consisting of all χ which are trivial on $C_0^{(e,q)}$. Thus, the computations needed to show whether a candidate subset $D = \bigcup_{i \in I} C_i^{(e,q)}$ is a connection set of a strongly regular Cayley graph are essentially reduced to evaluating Gauss sums. However, as previously said, evaluating Gauss sums explicitly is very difficult. In Section 3 of this paper, we will give a construction of strongly regular graphs by “lifting” a cyclotomic srg. To prove that our construction indeed gives rise to srgs, we do not evaluate the Gauss sums involved; instead, we use the Davenport-Hasse lifting formula stated below.

Theorem 2.2. ([3]) *Let χ be a nontrivial multiplicative character of $\mathbb{F}_q = \mathbb{F}_{p^f}$ and let χ' be the lift of χ to $\mathbb{F}_{q'} = \mathbb{F}_{p^{fs}}$, i.e., $\chi'(\alpha) = \chi(\text{Norm}_{q'/q}(\alpha))$ for $\alpha \in \mathbb{F}_{q'}$, where $s \geq 2$ is an integer. Then*

$$G_{fs}(\chi') = (-1)^{s-1} (G_f(\chi))^s.$$

3 Lifting cyclotomic strongly regular graphs via subdifference sets

In this section, we give a construction of strongly regular Cayley graphs by “lifting” a cyclotomic strongly regular graph via a subdifference set of the Singer difference sets. We start by reviewing a construction of the Singer difference sets.

Let p be a prime, $f \geq 1$, $m \geq 3$ be integers and $q = p^f$. Let L be a complete system of coset representatives of \mathbb{F}_q^* in $\mathbb{F}_{q^m}^*$. We may assume that L is chosen in such a way that $\text{Tr}_{q^m/q}(x) = 0$ or 1 for any $x \in L$. Let

$$L_0 = \{x \in L \mid \text{Tr}_{q^m/q}(x) = 0\} \text{ and } L_1 = \{x \in L \mid \text{Tr}_{q^m/q}(x) = 1\}.$$

Then,

$$H_0 = \{\bar{x} \in \mathbb{F}_{q^m}^*/\mathbb{F}_q^* \mid x \in L_0\} \quad (3.1)$$

is a Singer difference set.

Note that any nontrivial multiplicative character χ of exponent $(q^m - 1)/(q - 1)$ of $\mathbb{F}_{q^m}^*$ induces a character of the quotient group $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$, which will be denoted by χ also. Moreover, every character of $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ arises in this way. By a result of Yamamoto [28], for any nontrivial multiplicative character χ of exponent $(q^m - 1)/(q - 1)$ of $\mathbb{F}_{q^m}^*$, we have

$$\chi(H_0) = G_{fm}(\chi)/q.$$

Now, let $\mathbb{F}_q^* \leq C_0(= C_0^{(e, q^m)}) \leq \mathbb{F}_{q^m}^*$ be a subgroup such that $[\mathbb{F}_{q^m}^* : C_0] = e$. Then

$$\overline{C_0} = C_0/\mathbb{F}_q^* \leq \mathbb{F}_{q^m}^*/\mathbb{F}_q^*.$$

Let S be a complete system of coset representatives of $\overline{C_0}$ in $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$, and $G = \{\bar{s} \mid s \in S\} \simeq \mathbb{F}_{q^m}^*/C_0$. Then, by assumption, $[\mathbb{F}_{q^m}^* : C_0]$ divides $(q^m - 1)/(q - 1)$, i.e., $e = |G| \mid (q^m - 1)/(q - 1)$.

From now on, we assume that $\text{Cay}(\mathbb{F}_{q^m}, C_0)$ is strongly regular. Then $|H_0 \cap s\overline{C_0}|$, $s \in S$, take exactly two values. (See [7] or [26].) It follows that $|H_0 \cap s\overline{C_0}| - |H_0 \cap \overline{C_0}| = 0$ or δ , where δ is a nonzero integer. For any nontrivial multiplicative character χ of $\mathbb{F}_{q^m}^*$ of exponent e , we have

$$\begin{aligned} \chi(H_0) &= \sum_{s \in S} |H_0 \cap s\overline{C_0}| \chi(\bar{s}) \\ &= \sum_{s \in S} (|H_0 \cap s\overline{C_0}| - |H_0 \cap \overline{C_0}|) \chi(\bar{s}) \\ &= \delta \sum_{s \in S'} \chi(\bar{s}), \end{aligned}$$

where

$$S' = \{s \in S \mid |H_0 \cap s\overline{C_0}| - |H_0 \cap \overline{C_0}| = \delta\}. \quad (3.2)$$

Thus

$$\sum_{s \in S'} \chi(\bar{s}) = \frac{\chi(H_0)}{\delta} = \frac{G_{fm}(\chi)}{\delta q}. \quad (3.3)$$

It follows that δ is a power of p , and $\overline{S'} := \{\bar{s} \mid s \in S'\} \subset G$ is a $(e, |S'|, \lambda')$ -difference set, which is usually called a *subdifference set* of H_0 . See Section 6 of [26]. The term “subdifference set” was first introduced by McFarland [24].

Let γ be a primitive element of $\mathbb{F}_{q^{2m}}$ and let $\omega = \text{Norm}_{q^{2m}/q^m}(\gamma) = \gamma^{q^m+1}$, which is a primitive element of the subfield \mathbb{F}_{q^m} of $\mathbb{F}_{q^{2m}}$. Let $C_j^{(e, q^{2m})} = \gamma^j \langle \gamma^e \rangle$ and $C_j^{(e, q^m)} = \omega^j \langle \omega^e \rangle = \omega^j C_0$.

Theorem 3.1. *Assume that $\mathbb{F}_q^* \leq C_0 \leq \mathbb{F}_{q^m}^*$ be a subgroup such that $[\mathbb{F}_{q^m}^* : C_0] = e$, $-C_0 = C_0$, and $\text{Cay}(\mathbb{F}_{q^m}, C_0)$ is strongly regular. Let $I = \{0 \leq i \leq e - 1 \mid \bar{\omega}^i \in S'\}$, where S' is defined in (3.2) and $\bar{\omega}$ stands for $\omega\mathbb{F}_q^*$. Let*

$$D = \bigcup_{i \in I} C_i^{(e, q^{2m})}.$$

Then $\text{Cay}(\mathbb{F}_{q^{2m}}, D)$ is also strongly regular.

Proof: Let ψ_1 be the canonical additive character of $\mathbb{F}_{q^{2m}}$ and let χ'_e be a multiplicative character of order e of $\mathbb{F}_{q^{2m}}$. The restricted eigenvalues of $\text{Cay}(\mathbb{F}_{q^{2m}}, D)$ are $\psi_1(\gamma^a D)$, $0 \leq a \leq e-1$. By (2.2), in order to show that $\text{Cay}(\mathbb{F}_{q^{2m}}, D)$ is strongly regular, we compute the sums

$$T_a = e \cdot \psi_1(\gamma^a D) + |I| = \sum_{x=1}^{e-1} G_{2fm}(\chi_e'^{-x}) \sum_{i \in I} \chi_e'^x(\gamma^{a+i}),$$

where $a = 0, 1, \dots, e-1$. Since $e \mid (q^m - 1)$, χ_e' must be the lift of a character, say χ_e , of \mathbb{F}_{q^m} . By the Davenport-Hasse lifting formula, we have

$$T_a = - \sum_{x=1}^{e-1} \chi_e^x(\omega^a) G_{fm}(\chi_e^{-x}) G_{fm}(\chi_e^{-x}) \sum_{i \in I} \chi_e^x(\omega^i)$$

By the definition of I , we have

$$\sum_{i \in I} \chi_e^x(\omega^i) = \sum_{s \in S'} \chi_e^x(s) = \frac{G_{fm}(\chi_e^x)}{\delta q}.$$

Hence

$$\begin{aligned} T_a &= -\frac{1}{\delta q} \sum_{x=1}^{e-1} \chi_e^x(\omega^a) G_{fm}(\chi_e^{-x}) G_{fm}(\chi_e^{-x}) G_{fm}(\chi_e^x) \\ &= -\frac{q^{m-1}}{\delta} \sum_{x=1}^{e-1} \chi_e^x(\omega^a) G_{fm}(\chi_e^{-x}), \end{aligned} \quad (3.4)$$

where in the last step we used the fact that $G_{fm}(\chi_e^x) G_{fm}(\chi_e^{-x}) = \chi_e^x(-1) q^m$. By the assumption that $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(e, q^m)})$ is strongly regular, we have $\sum_{x=1}^{e-1} \chi_e^x(\omega^a) G_{fm}(\chi_e^{-x})$, $a = 0, 1, \dots, e-1$, take exactly two values. We conclude that T_a , $0 \leq a \leq e-1$, take exactly two values too. Therefore $\text{Cay}(\mathbb{F}_{q^{2m}}, D)$ is also strongly regular. \square

Note that the set D has size $|D| = \frac{(q^m-1)}{e} |I| (q^m + 1)$. By applying Theorem 3.1 to the known cyclotomic srgs in the statement of Conjecture 1.2, we obtain a lot of strongly regular Cayley graphs. We first apply Theorem 3.1 to the semi-primitive examples. In this case, we have $|I| = |S'| = 1$ by [11, p. 23].

Corollary 3.2. *Let p be a prime, $e \geq 2$, $q^m = p^{2jr}$, where $m = 2jr$, $r \geq 2$, $e \mid (p^j + 1)$, and j is the smallest such positive integer. Then there exists an $(n^2, r(n+1), -n+r^2+3r, r^2+r)$ strongly regular Cayley graph with $n = q^m$ and $r = (q^m - 1)/e$.*

The proof is straightforward. We omit it. Next we apply Theorem 3.1 to the subfield examples.

Corollary 3.3. *Let q be a prime power, $m \geq 3$ a positive integer and a any positive divisor of m . Then there exists an $(n^2, r(n+1), -n+r^2+3r, r^2+r)$ strongly regular Cayley graph with $n = q^m$ and $r = q^{m-a} - 1$.*

Proof: We apply Theorem 3.1 to the subfield examples of cyclotomic srgs. We use the same notation as in the statement and proof of Theorem 3.1. Then, by [11, p. 23], we have $C_0 = \mathbb{F}_{q^a}^*$, $e = \frac{q^m-1}{q^a-1}$, $|I| = |S'| = \frac{q^{m-a}-1}{q^a-1}$, $\delta = q^{a-1}$ and the restricted eigenvalues of $\text{Cay}(\mathbb{F}_{q^m}, C_0)$ are -1 and $q^a - 1$. The corollary now follows by straightforward computations using (3.4). \square

Remark 3.4. *In the case where $q = 2$ and $a = 1$, the parameters of the strongly regular Cayley graphs obtained in Corollary 3.3 are*

$$(2^{2m}, (2^m + 1)(2^{m-1} - 1), 2^{m-1}(2^{m-1} - 1) - 2, 2^{m-1}(2^{m-1} - 1)).$$

Then, the set $D \cup \{0\}$ clearly forms a difference set with parameters $(2^{2m}, 2^{m-1}(2^m-1), 2^{m-1}(2^{m-1}-1))$, which is a Hadamard difference set in the elementary abelian 2-group of order 2^{2m} . This difference set was first discovered in [12, p. 105]. The corresponding bent function is a monomial quadratic bent function.

Finally, we apply Theorem 3.1 to the eleven sporadic examples of cyclotomic srgs. In this case, the values of $k := |S'|$ are given in [26, Table II].

Corollary 3.5. *There exists a $(q^2, r(q+1), \lambda, \mu)$ negative Latin square type strongly regular Cayley graph, where $r = k(q-1)/e$, in each of the following cases:*

$$(q, e, k) = (3^5, 11, 5), (5^9, 19, 9), (3^{12}, 35, 17), (7^9, 37, 9), (11^7, 43, 21), (17^{33}, 67, 33), \\ (3^{53}, 107, 53), (5^{18}, 133, 33), (41^{81}, 163, 81), (3^{144}, 323, 161), (5^{249}, 499, 249).$$

4 Strongly regular Cayley graphs from quadratic forms

Let V be an n -dimensional vector space over \mathbb{F}_q . A function $Q : V \rightarrow \mathbb{F}_q$ is called a *quadratic form* if

- (i) $Q(\alpha v) = \alpha^2 Q(v)$ for all $\alpha \in \mathbb{F}_q$ and $v \in V$,
- (ii) the function $B : V \times V \rightarrow \mathbb{F}_q$ defined by $B(u, v) = Q(u+v) - Q(u) - Q(v)$ is bilinear.

We say that Q is *nonsingular* if the subspace W of V with the property that Q vanishes on W and $B(v, w) = 0$ for all $v \in V$ and $w \in W$ is the zero subspace (equivalently, we say that Q is nonsingular if it can not be written as a form in fewer than n variables by any invertible linear change of variables). If \mathbb{F}_q has odd characteristic or V is even-dimensional over an even-characteristic field \mathbb{F}_q , then Q is nonsingular if and only if B is nondegenerate [8, p. 14]. But this is not necessarily true in general. Now assume that n is even if q is even and n is arbitrary otherwise. Then, $Q : V = \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ is a nonsingular quadratic form if and only if the associated polar form $B(x, y) = Q(x+y) - Q(x) - Q(y)$ is nondegenerate; the characters ϕ_b , $b \in V$, of $(V, +)$ defined by

$$\phi_b(x) = \psi_1(B(b, x)), \quad \forall x \in V, \quad (4.1)$$

where ψ_1 is the canonical additive character of \mathbb{F}_q , are all the complex characters of $(V, +)$. We can linearly extend the characters ϕ_b to the whole group ring $\mathbb{C}[V]$: for $A = \sum_{g \in V} a_g g \in \mathbb{C}[V]$, we define $\phi_b(A) = \sum_{g \in V} a_g \phi_b(g)$.

It is well known that a nonsingular quadratic form on $V = \mathbb{F}_q^n$, where n is even, is equivalent to either

$$x_1 x_2 + x_3 x_4 + \cdots + x_{n-1} x_n, \quad (4.2)$$

or

$$x_1 x_2 + x_3 x_4 + \cdots + x_{n-3} x_{n-2} + (a x_{n-1}^2 + b x_{n-1} x_n + c x_n^2), \quad (4.3)$$

where $a x_{n-1}^2 + b x_{n-1} x_n + c x_n^2$ is irreducible over \mathbb{F}_q .

A nonsingular quadratic form equivalent to (4.2) (resp. (4.3)) is called *hyperbolic* (resp. *elliptic*).

Lemma 4.1. ([20, Theorem 3.2]) *Let $q = p^f$, where p a prime and $f \geq 1$ is an integer, and let Q be a nonsingular quadratic form on $V = \mathbb{F}_q^n$ with $n = 2m$ even. Then*

$$\sum_{x \in V} \psi_1(Q(x)) = \epsilon q^m,$$

where $\epsilon = 1$ or -1 according as Q is hyperbolic or elliptic.

For each $u \in \mathbb{F}_q$, define $D_u = \{x \in V \mid Q(x) = u\}$, and we use the same D_u to denote the corresponding group ring element $\sum_{z \in D_u} z \in \mathbb{C}[V]$. For a subset X of \mathbb{F}_q , we write $D_X = \sum_{x \in X} D_x$, which is viewed as an element of $\mathbb{C}[V]$. Now, we give the following key lemma.

Lemma 4.2. *Let $q = p^f$ be a prime power and $n = 2m$ be an even positive integer. Let $Q : V = \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ be a nonsingular quadratic form. For any $e \mid (q-1)$, let $C_i^{(e,q)} = \omega^i \langle \omega^e \rangle$ and $C_i^{(e,q^2)} = \gamma^i \langle \gamma^e \rangle$, $0 \leq i \leq e-1$, denote the cyclotomic classes of order e of \mathbb{F}_q and \mathbb{F}_{q^2} , respectively, where γ is a fixed primitive element of \mathbb{F}_{q^2} and $\omega = \text{Norm}_{q^2/q}(\gamma)$. Then, for any $0 \neq b \in V$,*

$$\phi_b(D_{C_i^{(e,q)}}) = \begin{cases} -\epsilon q^{m-1} \frac{q-1}{e}, & \text{if } Q(b) = 0, \\ -\epsilon q^{m-1} \psi'_1(\gamma^{i+s} C_0^{(e,q^2)}), & \text{if } Q(b) \in C_s^{(e,q)} \text{ for } 0 \leq s \leq e-1, \end{cases}$$

and

$$\phi_b(D_0) = \begin{cases} \epsilon q^{m-1} (q-1), & \text{if } Q(b) = 0, \\ -\epsilon q^{m-1}, & \text{if } Q(b) \neq 0, \end{cases}$$

where $\epsilon = 1$ or -1 according as Q is hyperbolic or elliptic, ϕ_b is defined in (4.1), and ψ'_1 is the canonical additive character of \mathbb{F}_{q^2} .

Proof: We compute the values of $\phi_b(D_{C_i^{(e,q)}})$. For $b \in V \setminus \{0\}$, we have

$$\begin{aligned} q \cdot \phi_b(D_{C_i^{(e,q)}}) &= \sum_{y \in C_i^{(e,q)}} \sum_{x \in V} \chi_b(x) \sum_{u \in \mathbb{F}_q} \psi_1(u(Q(x) - y)) \\ &= \sum_{x \in V} \sum_{u \in \mathbb{F}_q} \psi_1(B(b, x) + uQ(x)) \psi_u(-C_i^{(e,q)}) \\ &= \sum_{x \in V} \sum_{u \in \mathbb{F}_q^*} \psi_1(B(b, x) + uQ(x)) \psi_u(-C_i^{(e,q)}) + \frac{q-1}{e} \sum_{x \in V} \psi_1(B(b, x)). \end{aligned}$$

Since $\sum_{x \in V} \psi_1(B(b, x)) = 0$ and $B(b, x) + uQ(x) = -u^{-1}Q(b) + uQ(x + u^{-1}b)$ for $u \in \mathbb{F}_q^*$, we have

$$q \cdot \phi_b(D_{C_i^{(e,q)}}) = \sum_{x \in V} \sum_{u \in \mathbb{F}_q^*} \psi_1(-u^{-1}Q(b) + uQ(x + u^{-1}b)) \psi_u(-C_i^{(e,q)}). \quad (4.4)$$

By Lemma 4.1, we obtain

$$\begin{aligned} q \cdot \phi_b(D_{C_i^{(e,q)}}) &= \epsilon q^m \sum_{u \in \mathbb{F}_q^*} \psi_1(-u^{-1}Q(b)) \psi_u(-C_i^{(e,q)}) \\ &= \epsilon q^m \sum_{a=0}^{e-1} \sum_{c=0}^{(q-1)/e-1} \psi_1(\omega^{-a-ce}Q(b)) \psi_1(\omega^{a+ce}C_i^{(e,q)}) \\ &= \epsilon q^m \sum_{a=0}^{e-1} \psi_1(\omega^{a+i}C_0^{(e,q)}) \sum_{c=0}^{(q-1)/e-1} \psi_1(\omega^{-a-ce}Q(b)) \\ &= \begin{cases} -\epsilon q^m \frac{q-1}{e}, & \text{if } Q(b) = 0, \\ \epsilon q^m \sum_{a=0}^{e-1} \psi_1(\omega^{a+i}C_0^{(e,q)}) \psi_1(\omega^{-a+s}C_0^{(e,q)}), & \text{if } Q(b) \in C_s^{(e,q)} \text{ for } 0 \leq s \leq e-1. \end{cases} \end{aligned}$$

Below we further prove that

$$\sum_{a=0}^{e-1} \psi_1(\omega^{a+i}C_0^{(e,q)}) \psi_1(\omega^{-a+s}C_0^{(e,q)}) = -\psi'_1(\gamma^{i+s}C_0^{(e,q^2)}).$$

Let χ'_e be a multiplicative character of order e of \mathbb{F}_{q^2} . Since $e \mid (q-1)$, χ'_e must be the lift of a character, say χ_e , of \mathbb{F}_q . Then, by the orthogonality of characters and the Davenport-Hasse lifting

formula on Gauss sums, we have

$$\begin{aligned}
& \sum_{a=0}^{e-1} \psi_1(\omega^{a+i} C_0^{(e,q)}) \psi_1(\omega^{-a+s} C_0^{(e,q)}) \\
&= \frac{1}{e^2} \sum_{x=0}^{e-1} \sum_{y=0}^{e-1} G_f(\chi_e^x) G_f(\chi_e^y) \chi_e^{-x}(\omega^i) \chi_e^{-y}(\omega^s) \left(\sum_{a=0}^{e-1} \chi_e^{-x+y}(\omega^a) \right) \\
&= \frac{1}{e} \sum_{x=0}^{e-1} G_f(\chi_e^x)^2 \chi_e^{-x}(\omega^{i+s}) \\
&= -\frac{1}{e} \sum_{x=0}^{e-1} G_{2f}(\chi_e'^x) \chi_e'^{-x}(\gamma^{i+s}) \\
&= -\psi'_1(\gamma^{i+s} C_0^{(e,q^2)}).
\end{aligned}$$

Similarly, for $b \in V \setminus \{0\}$, we have

$$q \cdot \phi_b(D_0) = \begin{cases} \epsilon q^m(q-1), & \text{if } Q(b) = 0, \\ -\epsilon q^m, & \text{if } Q(b) \neq 0. \end{cases}$$

The proof is now complete. \square

Now we give the main theorem of this section.

Theorem 4.3. *Let q be a prime power, $e > 1$ be an integer dividing $q-1$, and I be a subset of $\{0, 1, \dots, e-1\}$. Let γ be a fixed primitive element of \mathbb{F}_{q^2} and $\omega = \text{Norm}_{q^2/q}(\gamma)$. Let $C_i^{(e,q^2)} = \gamma^i \langle \gamma^e \rangle$ and $E = \bigcup_{i \in I} C_i^{(e,q)}$. Assume that $\text{Cay}(\mathbb{F}_{q^2}, \bigcup_{i \in I} C_i^{(e,q^2)})$ is a negative Latin square type srg. Then, for any nonsingular quadratic form $Q : V = \mathbb{F}_q^n \rightarrow \mathbb{F}_q$, where $n = 2m$, the Cayley graph $\text{Cay}(V, D_E)$ is strongly regular.*

Proof: By assumption, $\text{Cay}(\mathbb{F}_{q^2}, \bigcup_{i \in I} C_i^{(e,q^2)})$ is an srg of negative Latin square type. Its parameters are $(q^2, r(q+1), -q+r^2+3r, r^2+r)$, where $r = |I|(q-1)/e$. The restricted eigenvalues of this srg are r and $r-q$. It follows from Lemma 4.2 that $\phi_b(D_E) = \sum_{i \in I} \phi_b(D_{C_i^{(e,q)}})$, $b \in V \setminus \{0\}$, take exactly two values, namely $-\epsilon q^{m-1}|I|(q-1)/e$ and $-\epsilon q^{m-1}(|I|(q-1)/e - q)$. Thus $\text{Cay}(V, D_E)$ is strongly regular. \square

Remark 4.4. (i) Note that the srg $\text{Cay}(V, D_E)$ obtained in the above theorem is of Latin square type or negative Latin square type according as $\epsilon = 1$ or -1 . One can see that under the same assumptions as in Theorem 4.3, $\text{Cay}(V, D_E \cup (D_0 \setminus \{0\}))$ is also strongly regular since $\text{Cay}(\mathbb{F}_{q^2}, \bigcup_{\bar{I}} C_i^{(e,q^2)})$ is a negative Latin square type srg, where $\bar{I} = \{0, 1, \dots, e-1\} \setminus I$. Furthermore, it is well known that $\text{Cay}(V, D_0)$ is also strongly regular with Latin square type or negative Latin square type parameters according to $\epsilon = 1$ or -1 [7].

(ii) The most important condition in Theorem 4.3 is that $\text{Cay}(\mathbb{F}_{q^2}, \bigcup_{i \in I} C_i^{(e,q^2)})$ is strongly regular. This condition is trivially satisfied in the following case. Let $e = 2$ and $I = \{0\}$. Then, $\text{Cay}(\mathbb{F}_{q^2}, C_0^{(2,q^2)})$ is obviously strongly regular with negative Latin square parameters. Thus, the aforementioned condition is trivially satisfied. In this case, the srg $\text{Cay}(V, D_E)$ obtained from Theorem 4.3 is exactly the affine polar graph. We thus have recovered Theorem 1.3.

The strongly regular Cayley graphs obtained in Section 3 satisfy the assumptions of Theorem 4.3, namely, e divides $q-1$ and $\text{Cay}(\mathbb{F}_{q^2}, \bigcup_{i \in I} C_i^{(e,q^2)})$ is a negative Latin square type srg. Thus, we can use the srgs obtained in Section 3 as starters to obtain new ones. We first consider the semi-primitive case. Let p be a prime, $e > 2$, $q = p^{2jr}$, where $r \geq 1$, $e \mid (p^j + 1)$, and j is the smallest such positive integer. In this case, E is chosen as the dual of the semi-primitive cyclotomic strongly

regular Cayley graph $\text{Cay}(\mathbb{F}_q, C_0^{(e,q)})$. Then, $|E| = (q-1)/e$ by [11, p. 23]. (Here, replace q^m of Corollary 3.2 with q .) By applying Theorem 4.3 to srgs of Corollary 3.2, we have the following corollary.

Corollary 4.5. *Let p be a prime, $e > 2$, $q = p^{2jr}$, $r \geq 2$, $e \mid (p^j + 1)$, and j is the smallest such positive integer. Then there exists a $(q^{2m}, r(q^m - \epsilon), \epsilon q + r^2 - 3\epsilon r, r^2 - \epsilon r)$ strongly regular Cayley graph with $r = q^{m-1}(q-1)/e$.*

We have thus recovered Theorem 1.4. Next we consider the subfield case. Let $q = p^{st}$ and $e = \frac{p^{st}-1}{p^s-1}$. Here, E is chosen as the dual of the subfield cyclotomic strongly regular Cayley graph $\text{Cay}(\mathbb{F}_q, C_0^{(e,q)})$. Then, $|E| = p^{s(t-1)} - 1$ by [11, p. 23]. (We replaced $n = q^m$ and $r = q^{m-a} - 1$ in Corollary 3.3 with $n = p^{st}$ and $r = p^{s(t-1)} - 1$ respectively.) Then, we have the following corollary.

Corollary 4.6. *There exists a $(p^{2stm}, (p^{stm} - \epsilon)r, \epsilon p^{stm} + r^2 - 3\epsilon r, r^2 - \epsilon r)$ strongly regular Cayley graphs for any prime p and positive integers s, t , and m , where $\epsilon = \pm 1$ and $r = p^{st(m-1)}(p^{s(t-1)} - 1)$.*

Finally, we consider the sporadic cases. Let q, e and k be as those in Corollary 3.5. In this case, E is chosen as the dual of sporadic cyclotomic strongly regular Cayley graphs $\text{Cay}(\mathbb{F}_q, C_0^{(e,q)})$. Then, $|E| = \frac{(q-1)}{e} \cdot k$. (Note that the number k is the size of the subdifference set corresponding to the cyclotomic srg $\text{Cay}(\mathbb{F}_q, C_0^{(e,q)})$, see [26, Table II].) Hence, we obtain the following corollary.

Corollary 4.7. *There exists a $(q^{2m}, r(q^m - \epsilon), \epsilon q^m + r^2 - 3\epsilon r, r^2 - \epsilon r)$ strongly regular Cayley graph for any $m \geq 1$, where $\epsilon = \pm 1$ and $r = q^{m-1} \cdot \frac{(q-1)}{e} \cdot k$, in each of the following cases:*

$$(q, e, k) = (3^5, 11, 5), (5^9, 19, 9), (3^{12}, 35, 17), (7^9, 37, 9), (11^7, 43, 21), (17^{33}, 67, 33) \\ (3^{53}, 107, 53), (5^{18}, 133, 33), (41^{81}, 163, 81), (3^{144}, 323, 161), (5^{249}, 499, 249).$$

5 Remarks on association schemes

The results on srgs obtained in Section 4 have implications on association schemes. Let X be a finite set. A (symmetric) *association scheme* with d classes on X consists of sets (binary relations) R_0, R_1, \dots, R_d which partition $X \times X$ and satisfy

- (1) $R_0 = \{(x, x) \mid x \in X\}$;
- (2) R_i is symmetric for all i ;
- (3) for any $i, j, k \in \{0, 1, \dots, d\}$ there is an integer $p_{i,j}^k$ such that given any pair $(x, y) \in R_k$

$$|\{z \in X \mid (x, z) \in R_i, (z, y) \in R_j\}| = p_{i,j}^k.$$

Note that each of the symmetric relations R_i can be viewed as an undirected graph $G_i = (X, R_i)$. Then, the graphs G_i , $1 \leq i \leq d$, decompose the complete graph with vertex set X . An srg with vertex set X and its complement form an association scheme on X with two classes. If $p_{i,j}^k = p_{j,i}^k$ for all i, j, k , then the association scheme is said to be *commutative*.

Let $(X, \{R_i\}_{i=0}^d)$ be a commutative association scheme. For each i , $0 \leq i \leq d$, let A_i denote the adjacency matrix of $G_i = (X, R_i)$. Then $A_i A_j = \sum_{k=0}^d p_{i,j}^k A_k$ and $A_i A_j = A_j A_i$, for all $0 \leq i, j \leq d$. It follows that A_0, A_1, \dots, A_d generate a commutative algebra (over the reals) of dimension $d+1$, which is called the *Bose-Mesner algebra* of the scheme $(X, \{R_i\}_{i=0}^d)$. The Bose-Mesner algebra has a unique set of primitive idempotents $E_0 = (1/|X|)J$, E_1, \dots, E_d , where J is

the all-ones matrix. Thus, the algebra has two basis, $\{A_i \mid 0 \leq i \leq d\}$ and $\{E_i \mid 0 \leq i \leq d\}$. We denote by P the base-change matrix such that

$$(A_0, A_1, \dots, A_d) = (E_0, E_1, \dots, E_d) \cdot P.$$

The entries in the i th column of P are the eigenvalues of A_i , $0 \leq i \leq d$. The matrix P is called the *first eigenmatrix* (or *character table*) of the association scheme.

Given a d -class commutative association scheme $(X, \{R_i\}_{0 \leq i \leq d})$, we can take union of classes to form graphs with larger edge sets (this process is called a *fusion*). It is not necessarily guaranteed that the fused collection of graphs will again form an association scheme on X . If an association scheme has the property that any of its fusions is also an association scheme, then we call the association scheme *amorphic*. A well-known and important example of amorphic association schemes is given by the cyclotomic association schemes on \mathbb{F}_q when the cyclotomy is uniform [2]. For a partition $\Lambda_0 = \{0\}$, $\Lambda_1, \dots, \Lambda_{d'} \subseteq \{1, 2, \dots, d\}$, let $R_{\Lambda_i} = \bigcup_{k \in \Lambda_i} R_k$. The following simple criterion, called the *Bannai-Muzychuk criterion*, is very useful for deciding whether $(X, \{R_{\Lambda_i}\}_{i=0}^{d'})$ forms an association scheme or not. Let P be the first eigenmatrix of the association scheme $(X, \{R_i\}_{i=0}^d)$. Then, $(X, \{R_{\Lambda_i}\}_{i=0}^{d'})$ forms an association scheme if and only if there exists a partition Δ_i , $0 \leq i \leq d'$, of $\{0, 1, \dots, d\}$, with $\Delta_0 = \{0\}$ such that each (Δ_i, Λ_j) -block of P has a constant row sum. Moreover, the constant row sum of the (Δ_i, Λ_j) -block is the (i, j) entry of the first eigenmatrix of the fusion scheme. (For a proof, see [1].)

From now on, we use the same notation and assumptions as those in Lemma 4.2. Let $G_i = \text{Cay}(V, T_i)$, where $T_i = \{i, -i\} \in V^*/\{1, -1\}$, and $R_0 = \{(x, x) \mid x \in V\}$, $R_i = E(\text{Cay}(V, T_i))$. Then, it is obvious that $(V, \{R_i\}_{i=0}^{|V^*/\{1, -1\}|})$ forms a commutative association scheme. Let P be the first eigenmatrix of this scheme. The (i, j) entry of the principal part of P (the matrix obtained by removing the first row and column from P) of the scheme is given by $\chi_i(T_j)$, where both the rows and columns are labeled by the elements of $V^*/\{1, -1\}$. Write $E_1 = D_0 \setminus \{0\}$ and $E_{s+2} = D_{C_s^{(e,q)}}$, where D_0 and $D_{C_s^{(e,q)}}$ are defined by $D_0 = \{x \in V \mid Q(x) = 0\}$ and $D_{C_s^{(e,q)}} = \{x \in V \mid Q(x) \in C_s^{(e,q)}\}$. Since $E_i = -E_i$ for $1 \leq i \leq e+1$, the subsets $(\Lambda_i = \Delta_i :=) E_i/\{1, -1\} \subseteq V^*/\{1, -1\}$, $1 \leq i \leq e+1$, are well defined. Then, the row sums of the (Δ_i, Λ_j) -block are given by $\chi_b(E_j)$, $b \in E_i$. On the other hand, Lemma 4.2 implies that for each pair i, j , the sum $\chi_b(E_j)$ are constant for all $b \in E_i$. Thus, by the Bannai-Muzychuk criterion, the partition gives a fusion scheme of $(V, \{R_i\}_{i=0}^{|V^*/\{1, -1\}|})$. In summary, we have the following result.

Theorem 5.1. *Let $q = p^f$ be a prime power and $n = 2m$ be an even positive integer. Let $Q : V = \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ be a nonsingular quadratic form. For any $e \mid (q-1)$, let $C_i^{(e,q)} = \omega^i \langle \omega^e \rangle$, $0 \leq i \leq e-1$, denote the cyclotomic classes of order e of \mathbb{F}_q . Then the decomposition of the complete graph on V by $\text{Cay}(V, D_0 \setminus \{0\})$ and $\text{Cay}(V, D_{C_i^{(e,q)}})$, $0 \leq i \leq e-1$, gives a $(e+1)$ -class association scheme.*

Next, we give a general sufficient condition for a fusion of the association scheme in Theorem 5.1 to be an association scheme.

Theorem 5.2. *Let $q = p^f$ be a prime power and $n = 2m$ be an even positive integer. Let $Q : V = \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ be a nonsingular quadratic form. For any $e \mid (q-1)$, let $C_i^{(e,q)} = \omega^i \langle \omega^e \rangle$ and $C_i^{(e,q^2)} = \gamma^i \langle \gamma^e \rangle$, $0 \leq i \leq e-1$, denote the cyclotomic classes of order e of \mathbb{F}_q . Assume that there exists a partition A_i , $1 \leq i \leq d$, of $\{i \mid 0 \leq i \leq e-1\}$ such that the decomposition of the complete graph of \mathbb{F}_{q^2} by $\text{Cay}(\mathbb{F}_q, \bigcup_{\ell \in A_i} C_\ell^{(e,q^2)})$, $1 \leq i \leq d$, is a fusion scheme of the e -class cyclotomic scheme on \mathbb{F}_{q^2} . Then, the decomposition of the complete graph on V by $\text{Cay}(V, D_0 \setminus \{0\})$ and $\text{Cay}(V, D_{\bigcup_{\ell \in A_i} C_\ell^{(e,q)}})$, $1 \leq i \leq d$, gives a $(d+1)$ -class association scheme.*

The above theorem follows immediately from Lemma 4.2. This can be seen as follows. By the assumption that the graph decomposition by $\text{Cay}(\mathbb{F}_{q^2}, \bigcup_{\ell \in A_i} C_\ell^{(e,q^2)})$, $1 \leq i \leq d$, gives a fusion

scheme of the e -class cyclotomic scheme on \mathbb{F}_{q^2} , there exists a partition Λ_h , $1 \leq h \leq d$, of $\{i \mid 0 \leq i \leq e-1\}$ such that for each $1 \leq h, i \leq d$, $\psi'_1(\gamma^s \cup_{\ell \in A_i} C_\ell^{(e, q^2)})$ are constant for all $s \in \Lambda_h$, i.e., $\phi_b(D_{\bigcup_{\ell \in A_i} C_\ell^{(e, q)}})$ are constant for all $b \in V$ such that $Q(b) \in \bigcup_{\ell \in \Lambda_h} C_\ell^{(e, q)}$ by Lemma 4.2. Similarly, $\phi_b(D_{\bigcup_{\ell \in A_i} C_\ell^{(e, q)}})$ are constant for all $b \in V$ such that $Q(b) = 0$. Furthermore, $\phi_b(D_0)$ is determined according to $Q(b) = 0$ or not. Thus, by the Bannai-Muzychuk criterion, the conclusion of Theorem 5.2 follows. We also remark that if the assumed association scheme of \mathbb{F}_{q^2} is amorphic, then so is the resulting scheme on V .

The condition of the above theorem is trivially satisfied in the following case. Let p be a prime, $e > 2$, $q = p^{2jr}$, $r \geq 2$, $e \mid (p^j + 1)$, and j is the smallest such positive integer. In this case, since the e -class cyclotomic association scheme on \mathbb{F}_{q^2} is amorphic, any fusion of the scheme in Theorem 5.1 forms an association scheme. This recovers Corollary 2.4 of [15]. Also, quite recently, an infinite family of (primitive and non-amorphic) three-class association schemes on $\mathbb{F}_{2^{6s}}$ satisfying the assumption of Theorem 5.2 was found [13, Theorem 7 (i)].

Finally, the following theorem of Van Dam [9] allows us to put the result of Theorem 4.3 in Section 4 in the context of association schemes.

Theorem 5.3. *Let $\{G_1, G_2, \dots, G_d\}$ be a decomposition of the complete graph on a set X , where each G_i is strongly regular. If G_i are all of Latin square type or all of negative Latin square type, then the decomposition is a d -class amorphic association scheme on X .*

By using Theorem 4.3 and part (i) of Remark 4.4 in conjunction with Theorem 5.3, we have the following:

Corollary 5.4. *Under the same assumptions as in Theorem 4.3, the strongly regular decomposition $\text{Cay}(V, D_E)$, $\text{Cay}(V, D_{\mathbb{F}_q^* \setminus E})$, $\text{Cay}(V, D_0 \setminus \{0\})$ yields a 3-class amorphic association scheme.*

Acknowledgments

The work of K. Momihara was supported by JSPS under Grant-in-Aid for Research Activity start-up 23840032. The work of Q. Xiang was done while he is a Program Officer at NSF. The views expressed here are not necessarily those of the NSF.

References

- [1] E. Bannai, Subschemes of some association schemes, *J. Algebra*, **144** (1991), 167–188.
- [2] L. D. Baumert, W. H. Mills, R. L. Ward, Uniform cyclotomy, *J. Number Theory*, **14** (1982), 67–82.
- [3] B. Berndt, R. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.
- [4] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Vol. I, 2nd edit., Cambridge University Press, 1999.
- [5] A. E. Brouwer, W. H. Haemers, *Spectra of Graphs*, Springer, Universitext, 2012.
- [6] A. E. Brouwer, R. M. Wilson, Q. Xiang, Cyclotomy and strongly regular graphs, *J. Alg. Combin.*, **10** (1999), 25–28.
- [7] R. Calderbank, W. M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.*, **18** (1986), 97–122.

- [8] P. J. Cameron, *Finite geometry and coding theory*, Lecture Notes for Socrates Intensive Programme, “Finite Geometries and Their Automorphisms,” Potenza, Italy, June 1999.
- [9] E. R. van Dam, Strongly regular decompositions of the complete graphs, *J. Alg. Combin.*, **17** (2003), 181–201.
- [10] J. A. Davis, Q. Xiang, Negative Latin square type partial difference sets in nonelementary abelian 2-groups, *J. London Math. Soc.*, **70** (2004), 125–141.
- [11] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Repts Suppl.*, No. 10, 1973.
- [12] J. F. Dillon, *Elementary Hadamard difference sets*, Ph.D. thesis, University of Maryland, 1974.
- [13] T. Feng, K. Momihara, Three-class association schemes from cyclotomy, [arXiv:1211.2864](#).
- [14] T. Feng, K. Momihara, Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, [arXiv:1201.0701](#).
- [15] T. Feng, B. Wen, Q. Xiang, J. Yin, Partial difference sets from quadratic forms and p -ary weakly regular bent functions, to appear in the proceedings of the conference in honor of Keqin Feng.
- [16] T. Feng, Q. Xiang, Strongly regular graphs from unions of cyclotomic classes, *J. Combin. Theory, Ser. B*, **102** (2012), 982–995.
- [17] G. Ge, Q. Xiang, T. Yuan, Construction of strongly regular Cayley graphs using index four Gauss sums, *J. Alg. Combin.*, DOI 10.1007/s10801-012-0368-y.
- [18] C. Godsil, G. Royle, *Algebraic Graph Theory*, GTM 207, Springer-Verlag, 2001.
- [19] C. L. M. de Lange, Some new cyclotomic strongly regular graphs, *J. Alg. Combin.*, **4** (1995), 329–330.
- [20] D. B. Leep, L. M. Schueller, Zeros of a pair of quadratic forms defined over a finite field, *Finite Fields Appl.*, **5** (1999), 157–176.
- [21] J. H. van Lint, A. Schrijver, Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields, *Combinatorica*, **1** (1981), 63–73.
- [22] S. L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.*, **4** (1994), 221–261.
- [23] R. J. McEliece, Irreducible cyclic codes and Gauss sums, in *Combinatorics*, pp. 183–200 (*Proc. NATO Advanced Study Inst., Breukelen, 1974; M. Hall, Jr. and J. H. van Lint (Eds.)*), Part 1, Math. Centre Tracts, Vol. 55, Math. Centrum, Amsterdam, 1974. Republished by Reidel, Dordrecht, 1975 (pp. 185–202).
- [24] R. L. McFarland, Sub-difference sets of Hadamard difference sets, *J. Combin. Theory, Ser. A*, **54** (1990), 112–122.
- [25] K. Momihara, Cyclotomic strongly regular graphs, skew Hadamard difference sets, and rationality of relative Gauss sums, *Europ. J. Combin.*, to appear.
- [26] B. Schmidt, C. White, All two-weight irreducible cyclic codes?, *Finite Fields Appl.*, **8** (2002), 321–367.
- [27] T. Storer, *Cyclotomy and Difference Sets*, Markham Publishing Company, 1967.
- [28] K. Yamamoto, On Jacobi sums and difference sets, *J. Combin. Theory, Ser. A*, **3** (1967), 146–181.

- [29] J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Ser. A*, **53** (2010), 2525–2542.